UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/591,151	11/13/2007	Yingxin Huang	HW 04107761US	6168

74365 7590 04/02/2010

Slater & Matsil, L.L.P.
17950 Preston Road, Suite 1000
Dallas, TX 75252

EXAMINER	
D AGOSTA, STEPHEN M	

ART UNIT	PAPER NUMBER
2617	

MAIL DATE	DELIVERY MODE
04/02/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/591,151	HUANG ET AL.	
	Examiner	Art Unit	
	Stephen M. D'Agosta	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6 and 11-19* is/are rejected.

7)☒ Claim(s) *7-10* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

Acknowledgment is made of applicant's claim for foreign priority based on an application filed in China on 6-25-2004.

It is noted, however, that applicant **has not filed** a certified copy of the this application (10-2004-0049883) as required by 35 U.S.C. 119(b).

Oath/Declaration

The applicant's claim to foreign priority in the OATH shows there is an application listed to which priority is claimed BUT the applicant has not checked the box stating if the certified copy has been provided (it has not, see above).

Drawings

Figures 1-3 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-6 and 11-19 rejected under 35 U.S.C. 103(a) as being unpatentable over AAPA and further in view of Gehrmann and Haverinen.

As per **claims 1 and 14,** Applicant's Admitted Prior Art (AAPA) teaches a method for managing a local Terminal Equipment (eg. laptop) accessing a network, wherein a management list containing an identity of the local TE is Configured in a Mobile Terminal and a user identity card is inserted in the MT (Figures 1-3 and page 4, L1-2 states that figure 3 is Prior Art access method: "*...Figure 3 is a schematic diagram illustrating a flowchart of a TE accessing the network using an USIM in the prior art.*"., the method comprising the steps of:

after receiving an authentication request identity message containing the identity of and from the local TE, the MT deciding whether to accept the request (figure 3 shows the Authentication Request Identity message from the network-side to the TE which is sent to the Mobile and an Acquire Status Identity is sent to the SIM card);

if a decision is made to accept the request, the MT acquiring an identity of the user identity card and returning the identity to the TE, the TE accessing the network using this identity, and the procedure is over and otherwise, refusing to return the identity of the user identity card to the TE, and terminating the procedure (Figure 3 culminates in the Mobile Accepting the identity request and returning an identity to the TE whereby the mobile/TE can access the network. Note that step 311 teaches either an accept/yes message or a failed/no message whereby the failure will result in termination/rejection. The examiner also notes that it would be inherent for a security

function to either allow or fail a user's access to a network, hence terminating the procedure is the only other possibility if the user is not authenticated properly);

but is silent on according to the information of the TE identity in the management list.

Gehrmann teaches a similar mobile-TE design whereby the mobile and TE authenticate with each other as based on a security/authentication procedure which is "key-based" (Abstract – note that Para #6 teaches that figure 4 shows a correlation between the mobile and which specific TE's it can authenticate to/with: [0064] Referring to FIG. 4, a subscription module or a RAA Client might have several different shared secrets. One particular shared secret is used to secure the communication with one particular RAA Client or subscription module respectively.). Note that figure 1 shows the mobile #106 and TE #101, figure 4 shows a "list" of ID's and Keys which are to be correlated/used while figure 5 shows specifically that a connection is established, identities are exchanged, keys are looked up and authentication is determined (which reads on using an identity listing).

Furthermore, **Haverinen** teaches a similar "split user equipment" security function whereby the mobile, TE and network authenticate each other in order for the mobile/TE to access the network (figures 1-3 and Para 9-10).

It would have been obvious to one skilled in the art at the time of the invention to modify the AAPA, such that access is according to the information of the TE identity in the management list, to provide a list of only authorized devices that can connect to the mobile for access to the network.

As per **claims 2 and 15,** the combo teaches Claim 1, wherein said management list containing the identity of the local TE comprises a management list of TEs allowed to access; and wherein the deciding method comprises:

the MT deciding whether the identity in the received request message exists in the management list of TEs allowed to access (Gehrman, Para #64, figures 4-5 teache that the mobile looks up each TE to determine if it is contained in its list and if authentication should be performed: [0064] Referring to FIG. 4, a subscription module or a RAA Client might have several different shared secrets. One particular shared secret is used to secure the communication with one particular RAA Client or subscription module respectively.);

if the identity exists in the management list, the MT acquiring the identity of the user identity card and returning the identity to the TE, the TE accessing the network using this identity, and the procedure is over; otherwise refusing to return the identity of the user identity card to the TE and terminating the procedure, or determining according to a policy of the user whether to return the identity of the user identity card to the TE (The AAPA, Figure 3 also shows the authentication process which is either allowed or failed/rejected, which reads on the claim) .

With further regard to claim 15, the prior art also teaches exchanging keys (see Gehrmann, figure 6).

As per **claims 3-4 and 17,** the combo teaches claim 1/14, wherein said management list containing the identity of the local TE comprises a management list of TEs (See Gehrmann figures 4-5 which show a list of accepted TE's) **but is silent on** forbidden to access; and wherein the deciding method comprises: the MT deciding whether the identity in the received request message exists in the management list of TEs forbidden to access; if the identity exists in the management list, refusing to return the identity of the user identity card to the TE and terminating the procedure, otherwise, determining according to a policy of the user whether to return the identity of the user identity card to the TE.

The examiner notes that Gehrmann teaches only accepted TE's with which the mobile can authenticate with but not "forbidden" TE's. By default, any TE not in the listing of figure 4 will be "forbidden" and hence not authenticated (eg. rejected).

The examiner takes **Official Notice** that one skilled would either a) reject any TE not on the listing (as per Gehrmann's figure 4) or also b) provide a listing of forbidden TE's.

It would have been obvious to one skilled in the art at the time of the invention to modify the combo, such that forbidding access; and wherein the deciding method comprises: the MT deciding whether the identity in the received request message exists in the management list of TEs forbidden to access; if the identity exists in the management list, refusing to return the identity of the user identity card to the TE and terminating the procedure, otherwise, determining according to a policy of the user whether to return the identity of the user identity card to the TE, to provide means for only allowing verified users who are contained in the listing while forbidding any on the forbidden listing.

With further regard to claim 4, the prior art also reads on allowed/forbidden lists, acquiring user identity card and returning it to the TE for access to the network and/or refusing to return the identify if a request is from a forbidden TE.

As per **claims 5, 16 and 18,** the combo teaches Claim 2/14/4, wherein the authentication request identity message comprises information of the authority identifier of the service to be requested, the method further comprising the steps of: setting in the management list of TEs allowed to access authority information for TE to access the network; after deciding according to the information of TE identity in the management list to accept the authentication identity request, the MT deciding whether the information of service authority identifier in the received request message is consistent with the authority information of the TE in the management list; if the information of service authority identifier in the authentication request identity message is consistent with the authority information in the management list of TEs allowed to access, the MT acquiring identity of the user identity card and returning the identity to the TE, the TE accessing the network using this identity, and the procedure is over; otherwise, refusing to return the identity of the user identity card to the TE, and terminating the procedure (Gehrmann teaches the mobile/TE authentication process to allow the user to access the network's "services", eg. voice, data, txt/SMS, etc. Note that access to the network inherently requires authentication with the HLR and AAA. The examiner takes **Official Notice** that an HLR/AAA would be consulted for network access authentication, otherwise the mobile/TE would be refused access).

As per **claims 6 and 19,** the combo teaches Claim 5/18, further comprising the steps of: setting current state information of the TE in the management list of TEs allowed to access; after receiving an authentication request identity message containing the TE identity from the local TE (see prior art above)

But is silent on when the network allows only a limited number of TEs to access the network via an MT AND the MT first deciding according to the current state information of the TE in the management list whether the MT itself is serving the number of TEs as limited by the network; if the MT is serving the number of TEs as limited by the network, refusing to return the identity of the user identity card to the TE, and terminating the procedure; otherwise, deciding according to the identity information of the TE whether to accept the request and continuing the subsequent steps.

The examiner takes **Official Notice** that a base station/cell can only provide a finite number of access channels, which "limits" the number of TE's that can access a network.

It would have been obvious to one skilled in the art at the time of the invention to modify the combo, such that when the network allows only a limited number of TEs to access the network via an MT AND the MT first deciding according to the current state information of the TE in the management list whether the MT itself is serving the number of TEs as limited by the network; if the MT is serving the number of TEs as limited by the network, refusing to return the identity of the user identity card to the TE, and terminating the procedure; otherwise, deciding according to the identity information of the TE whether to accept the request and continuing the subsequent steps, to provide means for accepting only a maximum number of mobile/TE's to access a cell site's channels.

As per **claim 11,** the combo teaches Claim 1, wherein the process of the TE accessing the network using the identity comprises:

the TE making an authentication with the network side using the identity, and receiving the authentication response message from the network side; the TE deciding whether the received authentication response message is a message of successful authentication; if the received authentication response message is a message of successful authentication, the TE sending a notice of successful authentication to the MT, receiving key(s) information from the MT, and accessing the network using the received key(s) information; otherwise, terminating the procedure; or, the TE making authentication with the network side using the identity, and forwarding the received authentication response message from the network side to the MT; the MT deciding whether the received authentication response message is a message of successful authentication; if the received authentication response message is a message of successful authentication, the MT sending key(s) information to the TE, and the TE accessing the network using the received key(s) information; otherwise, terminating the procedure (See the AAPA as well as Gehrmann figures 4-6).

As per **claim 12,** the combo teaches Claim 1, wherein at least one management list is set in the MT, and each management list is corresponding to a user identity card (See AAPA and Gehrmann who teaches a listing of TE's and keys for the SIM).

As per **claim 13,** the combo teaches claim 12, wherein the user identity card comprises a Subscriber Identity Module (SIM) of GSM, a USIM of 3GPP, or an ISIM of IP multimedia subsystem (The AAPA, Gehrmann and Haverinen teach use of a SIM).

Allowable Subject Matter

Claims 7-10 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

These claims recite highly detailed design concepts not found in the prior art of record:

claim 7: "...wherein the TE accessing the network using the identity comprises the steps of: after sending the identity to the network side and receiving an authentication request from the network side, the TE acquiring an authentication response value via the MT, forwarding the response value to the network side, and receiving an authentication response message from the network side; the TE receiving a message of successful authentication from the network side, forwarding the message of successful authentication to the MT; after receiving the message of successful authentication from the network side forwarded by the TE, the MT modifying the current state information of the TE in the management list of TEs allowed to access, making the information indicate an online state, then sending key(s) information to the TE, and the TE accessing the network using the received key(s)information; or, after sending the identity to the network side and receiving an authentication request from the network side, the TE acquiring an authentication response value via the MT, sending the

authentication response value to the network side, and directly forwarding the received authentication response message from the network side to the MT; the MT, after deciding that a message of successful authentication is received from the network side, modifying the current state information of the TE in the management list of TEs allowed to access, making the information indicate an online state, then sending to the TE key(s) information, and the TE accessing the network using the received key(s) information".

claim 8 "...further comprising the steps of: after the TE terminating the service communication with the network side, the network side sending to the TE a logoff notice containing the authority identifier of logoff, the TE forwarding the received logoff notice to the MT, and the MT, after receiving the logoff notice forwarded by the TE, modifying the current state information of the TE in the management list of TEs allowed to access, making the information indicate an unused state".

claim 9: "...further comprising the steps of: when not having received a logoff notice sent from the TE that has been identified as in the online state for a preset period of time, the MT modifying the state information of this TE, making the information indicate the unused state".

claim 10: "...when the MT modifies the state information of the TE in the management list of TEs allowed to access to make the information indicate the online state, further comprising the steps of: stamping the time on the modified state information; wherein when the MT receives a new authentication identity request and decides according to the current state information of the TE in the management list that the MT itself is serving a number of TEs as limited by the network, the method further comprises: deciding whether the time difference between the current time and the time indicated by the time stamp on the state information of the TE has exceeded a preset time threshold; if the time difference has exceeded the preset time threshold, modifying the state information of the TE, and making the information indicate the unused state;

otherwise, refusing to return the identity of the user identity card to the TE, and terminating the procedure".

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Stephen M. D'Agosta whose telephone number is 571-272-7862. The examiner can normally be reached on M-F, 8am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lun Yi Lao can be reached on 571-272-7671. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Stephen M. D'Agosta/
Primary Examiner, Art Unit 2617